IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit for registering virus infected files which are stored on said disk;

a virus checker for detecting if a file stored on said disk is infected with a virus, wherein the virus checker is activated at intervals of a specific period or in response to a command instruction;

a table registering unit for registering a result of detection from said virus checker in said infection management table unit;

a judging unit for judging if a file is infected with a virus in response to an external use request externally made for a file stored on said disk by referencing said infection management table unit; and

a prohibiting unit for prohibiting use of the externally requested file when said judging unit judges that the externally requested file is infected with a virus.

2. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, wherein said virus checker is designed to be run by said storage device having the function of coping with a computer virus.

3. (withdrawn) A storage device having the function of coping with a computer virus according to claim 2, wherein said virus checker is designed to be activated at intervals of a specific period.

4. (withdrawn) A storage device having the function of coping with a computer virus according to claim 2, wherein said virus checker is designed to be activated in response to a command instruction.

5. (withdrawn) A storage device having the function of coping with a computer virus according to claim 2, wherein when a writing request is issued for a system startup area stored on said disk, said table registering unit judges that a file which is stored on said disk and is a source of the writing request is infected with a virus, and registers the fact in said infection management table unit.

6. (withdrawn) A storage device having the function of coping with a computer virus according to claim 5, further comprising an invalidating unit that when a writing request is issued for a system startup area stored on said disk, invalidates the writing request.

7. (withdrawn) A storage device having the function of coping with a computer virus according to claim 5, further comprising a determining unit for determining through interactive processing whether the use of a virus-infected file that is registered in said infection management table unit should be permitted, wherein said prohibiting unit does not prohibit the use of a file which is permitted by said determining unit.

8. (withdrawn) A storage device having the function of coping with a computer virus according to claim 5, further comprising a first managing unit for managing original information of files stored on said disk, a second managing unit for managing differential information brought about due to modification concerning the files stored on said disk and history information concerning the differential information brought about due to modification, and a file registering unit for merging original information of a file managed by said first managing unit with differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk.

9. (withdrawn) A storage device having the function of coping with a computer virus according to claim 5, further comprising a saving unit for saving a virus-infected file that is registered in said infection management table unit and virus information concerning the file in an inexecutable area, and a reading unit for reading information saved in said inexecutable area under the condition that permission information for permitting access to said inexecutable area is given.

10. (withdrawn) A storage device having the function of coping with a computer virus

according to claim 2, when a writing request is issued for an executable file stored on said disk, said table registering unit judges that a file which is stored on said disk and is a source of the writing request is infected with a virus, and registers the fact in said infection management table unit.

11. (withdrawn) A storage device having the function of coping with a computer virus according to claim 2, wherein when the size of a file is varied by running the file, said table registering unit judges that the file, said table registering unit judges that the file stored on said disk is infected with a virus, and registers the fact in said infection management table unit.

12. (withdrawn) A storage device having the function of coping with a computer virus according to claim 2, wherein although a file stored on said disk is judged to be an executable file in terms of the file name, if the file is declared to be a data file, said table registering unit judges that the file stored on said disk is infected with a virus, and registers the fact in said infection management table unit.

13. (withdrawn) A storage device having the function of coping with a computer virus according to claim 2, further comprising a determining unit for determining through interactive processing whether the use of a virus-infected file that is registered in said infection management table unit should be permitted, wherein said prohibiting unit does not prohibit the use of a file which is permitted by said determining unit.

14. (withdrawn) A storage device having the function of coping with a computer virus according to claim 25, further comprising an invalidating unit that when a writing request is issued for a system startup area stored on said disk, invalidates the writing request.

15. (withdrawn) A storage device having the function of coping with a computer virus according to claim 14, further comprising a dedicated writing unit for executing writing for a system startup area stored on said disk, wherein when a writing request is issued for the system startup area stored on said disk, if the writing request specifies the use of said writing unit, said invalidating unit does not invalidate the writing request.

16. (withdrawn) A storage device having the function of coping with a computer virus according to claim 2, further comprising a first managing unit for managing original information of

files stored on said disk, a second managing unit for managing differential information brought about due to modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification, and file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk.

17. (withdrawn) A storage device having the function of coping with a computer virus according to claim 2, further comprising a saving unit for saving a virus-infected file that is registered in said infection management table unit and virus information concerning the file in an inexecutable area, and a reading unit for reading information saved in said inexecutable area under the condition that permission information for permitting access to said inexecutable area is given.

18. (withdrawn) A storage device having the function of coping with a computer virus according to claim 26, further comprising a permitting unit for determining through interactive processing whether a writing request made for a file, which is registered as a virus-infected file by said table registering unit and is running, should be permitted.

19. (withdrawn) A storage device having the function of coping with a computer virus according to claim 18, wherein when a writing request is permitted by said permitting unit, if a file that is a destination of the writing request is rewritten, said table registering unit judges that the file which is stored on said disk and is the destination of the writing request is infected with a virus and registers the fact in said infection management table unit.

20. (withdrawn) A storage device having the function of coping with a computer virus according to claim 18, further comprising a determining unit for determining through interactive processing whether the use of a virus-infected file that is registered in said infection management table unit should be permitted, wherein said prohibiting unit does not prohibit the use of a file which is permitted by said determining unit.

21. (withdrawn) A storage device having the function of coping with a computer virus according to claim 18, further comprising a first managing unit for managing original information

of files stored on said disk, a second managing unit for managing differential information brought about due to modification concerning the files stored on said disk and history information concerning the differential information brought about due to modification, and a file registering unit for merging original information of a file managed by said first managing unit with differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk.

22. (withdrawn) A storage device having the function of coping with a computer virus according to claim 18, further comprising a saving unit for saving a virus-infected file that is registered in said infection management table unit and virus information concerning the file in an inexecutable area, and a reading unit for reading information saved in said inexecutable area under the condition that permission information for permitting access to said inexecutable area is given.

23. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, wherein said virus checker is designed to be activated at intervals of a specific period.

24. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, wherein said virus checker is designed to be activated in response to a command instruction.

25. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, wherein when a writing request is issued for a system startup area stored on said disk, said table registering unit judges that a file which is stored on said disk and is a source of the writing request is infected with a virus, and registers the fact in said infection management table unit.

26. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, wherein when a writing request is issued for an executable file stored on said disk, said table registering unit judges that a file which is stored on said disk and is a source of the writing request is infected with a virus, and registers the fact in said infection management table unit.

27. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, wherein when the size of a file is varied by running the file, said table registering unit judges that the file stored on said disk is infected with a virus, and registers the fact in said infection management table unit.

28. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, wherein although a file stored on said disk is judged to be an declared to be a data file, said table registering unit judges that the file stored on said disk is infected with a virus, and registers the fact in said infection management table unit.

29. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, further comprising a determining unit for determining through interactive processing whether the use of a virus-infected file that is registered in said infection management table unit should be permitted, wherein said prohibiting unit does not prohibit the use of a file which is permitted by said determining unit.

30. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, further comprising:

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification; and

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk,

wherein said first managing unit manages original information that is confirmed not to be infected with a virus by said virus checker, and said second managing unit manages differential information brought about due to modification which is confirmed not to be infected with a virus by said virus checker.

31. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, further comprising:

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification; and

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk,

wherein as for a file which is stored on said disk, of which original information is not registered in said first managing unit, and of which differential information brought about due to modification is not registered in said second managing unit, said table registering unit judges that the file stored on said disk is infected with a virus and registers the fact in said infection management table unit.

32. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, further comprising:

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification; and

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk,

wherein said first managing unit manages original information of said virus checker, and said second managing unit manages differential information brought about due to modification concerning said virus checker and history information concerning the differential information brought about due to modification.

33. (withdrawn) A storage device having the function of coping with a computer virus according to claim 32, wherein said generating unit generates said virus checker at the time of running said virus checker.

34. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, further comprising:

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification; and

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk,

wherein said first managing unit encodes and manages original information, and said second managing unit encodes and manages differential information brought about due to modification, further comprising a decoding unit for decoding encoded data managed by said first and second managing unit, and an encoding unit for executing inverse conversion that is inverse to conversion performed by said decoding unit.

35. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, further comprising:

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification;

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk; and

a saving unit for saving a virus-infected file that is registered in said infection management table unit and virus information concerning the file in an executable area, and a reading unit for reading information saved in said inexecutable area under the condition that permission information for permitting access to said inexecutable area is given.

36. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, further comprising:

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential

information brought about due to modification;

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk; and

a restoring unit for deleting a virus-infected file, which is registered in said infection management table unit, from said disk, activating said file registering unit, thus restoring the file, and then registering the restored file on said disk,

wherein said first managing unit encodes and manages original information, and said second managing unit encodes and manages original information, and said second managing unit encodes and manages differential information brought about due to modification, further comprising a decoding unit for decoding encoded data managed by said first and second managing units, and an encoding unit for executing inverse conversion that is inverse to conversion performed by said decoding unit.

37. (withdrawn) A storage device having the function of coping with a computer virus according to claim 1, further comprising:

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification;

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk;

a restoring unit for deleting a virus-infected file, which is registered in said infection management table unit, from said disk, activating said file registering unit, thus restoring the file, and then registering the restored file on said disk; and

a saving unit for saving a virus-infected file that is registered in said infection management table unit and virus information concerning the file in an inexecutable area, and a reading unit for reading information saved in said inexecutable area under the condition that permission information for permitting access to said inexecutable area is given.

38. (withdrawn) A storage device, having the function of coping with a computer

virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit used to manage files stored on said disk to see if the files are infected with viruses;

a table registering unit for receiving a result of detection from a virus checker for detecting if a file stored on said disk is infected with a virus, and for registering the result in said infection management table unit;

a judging unit that, when a use request is made externally for a file stored on said disk, references said infection management table unit so as to judge if the file is infected with a virus;

a prohibiting unit that, when said judging unit judges that a file is infected with a virus, prohibits the use of the file, wherein when a writing request is issued for a system startup area stored on said disk, said table registering unit judges that a file which is stored on said disk and is a source of the writing request is infected with a virus, and registers the fact in said infection management table unit; and

a file registering unit for merging original information of a file managed by a first managing unit with differential information brought about due to modification concerning a file which is managed by a second managing unit so as to produce a produced file, and for registering the produced file on said disk.

39. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit used to manage files stored on said disk to see if the files are infected with viruses;

a table registering unit for receiving a result of detection from a virus checker for detecting if a file stored on said disk is infected with a virus, and for registering the result in said infection management table unit;

a judging unit that, when a use request is made externally for a file stored on said disk, references said infection management table unit so as to judge if the file is infected with a virus;

a prohibiting unit that, when said judging unit judges that a file is infected with a virus, prohibits the use of the file;

a saving unit for saving a virus-infected table unit and virus information concerning the file in an inexecutable area;

a reading unit for reading information saved in said inexecutable area under the condition that permission information for permitting access to said inexecutable area is given; and

a file registering unit for merging original information of a file managed by a first

managing unit with differential information brought about due to modification concerning a file which is managed by a second managing unit so as to produce a produced file, and for registering the produced file on said disk.

40. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit used to manage files stored on said disk to see if the files are infected with viruses;

a table registering unit for receiving a result of detection from a virus checker for detecting if a file stored on said disk is infected with a virus, and for registering the result in said infection management table unit;

a judging unit that, when a use request is made externally for a file stored on said disk, references said infection management table unit so as to judge if the file is infected with a virus;

a prohibiting unit that, when said judging unit judges that a file is infected with a virus, prohibits the use of the file;

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification;

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a produced file, and for registering the produced file on said disk;

a restoring unit for deleting a virus-infected file, which is registered in said infection management table unit, from said disk, activating said file registering unit, thus restoring the file, and then registering the restored file on said disk.

41. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit used to manage files stored on said disk to see if the files are infected with viruses;

a table registering unit for internally receiving a result of detection from a virus checker which internally detects that a file stored on said disk is infected with a virus, and for registering the result in said infection management table unit;

a judging unit that, when a use request is made externally for a file stored on said disk, references said infection management table unit so as to judge if the file is infected with a virus;

a prohibiting unit that, when said judging unit judges that a file is infected with a virus, prohibits the use of the file; and

a file registering unit for merging original information of a file managed by a first managing unit with differential information brought about due to modification concerning a file which is managed by a second managing unit so as to produce a produced file, and for registering the produced file on said disk.

42. (withdrawn) A method of storing a computer program on a computer storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising the steps of:

managing files stored on said disk to see if the files are infected with viruses;

receiving a result of detection from a virus checker for detecting if a file stored on said disk is infected with a virus;

registering the result of detection;

referencing said infection management table unit so as to judge if the file is infected with a virus when a use request is made externally for a file stored on said disk;

prohibiting the use of the file when judging that a file is infected with a virus;

judging that a stored file on said disk is a source of the use request infected with a virus and registering when the use request is issued for a system startup area stored on said disks;

merging original information of a file managed by a first managing unit with differential information brought about due to modification concerning a file which is managed by a second managing unit so as to produce a produced file; and

registering the produced file on said disk.

43. (withdrawn) A method of storing a computer program on a computer storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising the steps of:

managing files stored on said disk to see if the files are infected with viruses;

receiving a result of detection from a virus checker for detecting if a file stored on said disk is infected with a virus;

registering the result of detection;

judging if the file is infected with a virus when a use request is made externally for a file

stored on said disk;

prohibiting use of the infected file when judging that a file is infected with a virus;

saving a virus-infected table and virus information concerning the file in an inexecutable area;

reading information saved in said inexecutable area under the condition that permission information for permitting access to said inexecutable area is given;

merging original information of a file managed by a first managing unit with differential information brought about due to modification concerning a file which is managed by a second managing unit so as to produce a produced file; and

registering the produced file on said disk.

44. (withdrawn) A method of storing a computer program on a computer storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising the steps of:

managing files stored on said disk to see if the files are infected with viruses;

receiving a result of detection from a virus checker for detecting if a file stored on said disk is infected with a virus;

registering the result of detection;

judging if the file is infected with a virus when a use request is made externally for a file stored on said disk;

prohibiting the use of the file when judging that a file is infected with a virus;

managing original information of files stored on said disk;

managing differential information brought about by modification concerning the files stored on said disk and history information concerning said differential information brought about due to the modification;

merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a produced file;

registering the produced file on said disk;

deleting a registered virus-infected file from said disk, thus restoring the file; and

registering the restored file on said disk.

45. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit for registering virus infected files which are stored on said disk;

a virus checker for detecting if a file stored on said disk is infected with a virus, wherein the virus checker is activated at intervals of a specific period or in response to a command instruction;

a table registering unit for registering a result of detection from said virus checker in said infection management table unit;

a judging unit for judging if a file is infected with a virus in response to an external use request externally made for a file stored on said disk by referencing said infection management table unit;

a prohibiting unit for prohibiting use of the externally requested file when said judging unit judges that the externally requested file is infected with a virus;

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification; and

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk,

wherein said first managing unit manages original information that is confirmed not to be infected with a virus by said virus checker, and said second managing unit manages differential information brought about due to modification which is confirmed not to be infected with a virus by said virus checker.

46. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit for registering virus infected files which are stored on said disk;

a virus checker for detecting if a file stored on said disk is infected with a virus, wherein the virus checker is activated at intervals of a specific period or in response to a command instruction;

a table registering unit for registering a result of detection from said virus checker in said infection management table unit;

a judging unit for judging if a file is infected with a virus in response to an external use request externally made for a file stored on said disk by referencing said infection management table unit;

a prohibiting unit for prohibiting use of the externally requested file when said judging unit judges that the externally requested file is infected with a virus;

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification; and

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk,

wherein as for a file which is stored on said disk, of which original information is not registered in said first managing unit, and of which differential information brought about due to modification is not registered in said second managing unit, said table registering unit judges that the file stored on said disk is infected with a virus and registers the fact in said infection management table unit.

47. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit for registering virus infected files which are stored on said disk;

a virus checker for detecting if a file stored on said disk is infected with a virus, wherein the virus checker is activated at intervals of a specific period or in response to a command instruction;

a table registering unit for registering a result of detection from said virus checker in said infection management table unit;

a judging unit for judging if a file is infected with a virus in response to an external use request externally made for a file stored on said disk by referencing said infection management table unit;

a prohibiting unit for prohibiting use of the externally requested file when said judging unit judges that the externally requested file is infected with a virus;

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification; and

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk,

wherein said first managing unit manages original information of said virus checker, and said second managing unit manages differential information brought about due to modification concerning said virus checker and history information concerning the differential information brought about due to modification.

48. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit for registering virus infected files which are stored on said disk;

a virus checker for detecting if a file stored on said disk is infected with a virus, wherein the virus checker is activated at intervals of a specific period or in response to a command instruction;

a table registering unit for registering a result of detection from said virus checker in said infection management table unit;

a judging unit for judging if a file is infected with a virus in response to an external use request externally made for a file stored on said disk by referencing said infection management table unit;

a prohibiting unit for prohibiting use of the externally requested file when said judging unit judges that the externally requested file is infected with a virus;

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification; and

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk,

wherein said first managing unit encodes and manages original information, and said second managing unit encodes and manages differential information brought about due to modification, further comprising a decoding unit for decoding encoded data managed by said first and second managing unit, and an encoding unit for executing inverse conversion that is inverse to conversion performed by said decoding unit.

49. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit for registering virus infected files which are stored on said disk;

a virus checker for detecting if a file stored on said disk is infected with a virus, wherein the virus checker is activated at intervals of a specific period or in response to a command instruction;

a table registering unit for registering a result of detection from said virus checker in said infection management table unit;

a judging unit for judging if a file is infected with a virus in response to an external use request externally made for a file stored on said disk by referencing said infection management table unit;

a prohibiting unit for prohibiting use of the externally requested file when said judging unit judges that the externally requested file is infected with a virus;

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification;

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk; and

a saving unit for saving a virus-infected file that is registered in said infection management table unit and virus information concerning the file in an executable area, and a reading unit for reading information saved in said inexecutable area under the condition that permission information for permitting access to said inexecutable area is given.

50. (withdrawn) A storage device, having the function of coping with a computer

virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit for registering virus infected files which are stored on said disk;

a virus checker for detecting if a file stored on said disk is infected with a virus, wherein the virus checker is activated at intervals of a specific period or in response to a command instruction;

a table registering unit for registering a result of detection from said virus checker in said infection management table unit;

a judging unit for judging if a file is infected with a virus in response to an external use request externally made for a file stored on said disk by referencing said infection management table unit;

a prohibiting unit for prohibiting use of the externally requested file when said judging unit judges that the externally requested file is infected with a virus;

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification;

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk;

a restoring unit for deleting a virus-infected file, which is registered in said infection management table unit, from said disk, activating said file registering unit, thus restoring the file, and then registering the restored file on said disk,

wherein said first managing unit encodes and manages original information, and said second managing unit encodes and manages original information, and said second managing unit encodes and manages differential information brought about due to modification, further comprising a decoding unit for decoding encoded data managed by said first and second managing unit, and an encoding unit for executing inverse conversion that is inverse to conversion performed by said decoding unit.

51. (withdrawn) A storage device, having the function of coping with a computer virus, which has the ability to deal with infection of a file stored on a disk with a virus, comprising:

an infection management table unit for registering virus infected files which are stored on

said disk;

a virus checker for detecting if a file stored on said disk is infected with a virus, wherein the virus checker is activated at intervals of a specific period or in response to a command instruction;

a table registering unit for registering a result of detection from said virus checker in said infection management table unit;

a judging unit for judging if a file is infected with a virus in response to an external use request externally made for a file stored on said disk by referencing said infection management table unit;

a prohibiting unit for prohibiting use of the externally requested file when said judging unit judges that the externally requested file is infected with a virus;

a first managing unit for managing original information of files stored on said disk;

a second managing unit for managing differential information brought about modification concerning the files stored on said disk and history information concerning said differential information brought about due to modification;

a file registering unit for merging the original information of a file managed by said first managing unit with the differential information brought about due to modification concerning the file which is managed by said second managing unit so as to produce a file, and for registering the produced file on said disk;

a restoring unit for deleting a virus-infected file, which is registered in said infection management table unit, from said disk, activating said file registering unit, thus restoring the file, and then registering the restored file on said disk; and

a saving unit for saving a virus-infected file that is registered in said infection management table unit and virus information concerning the file in an inexecutable area, and a reading unit for reading information saved in said inexecutable area under the condition that permission information for permitting access to said inexecutable area is given.

52. (withdrawn) A data processing system which has the ability to deal with infection of a file with a virus, the system comprising:

a storage device storing files;

a virus scanner detecting if a file stored in said storage device is infected with a virus; and

a saving unit saving a detected virus-infected file into a specific area within said storage device.

53. (withdrawn) A data processing system according to claim 52, further comprising a managing unit managing the detected virus-infected file that is saved in the specific area.

54. (withdrawn) A data processing system according to claim 53, further comprising a deleting unit deleting the detected virus-infected file.

55. (withdrawn) A data processing system according to claim 52, further comprising an encoder unit encrypting the detected virus-infected file.

56. (withdrawn) A data processing system according to claim 52, wherein the virus-infected file saved in the specific area is not able to run.

57. (withdrawn) A method for dealing with infection of a file by a virus, the method comprising:

storing files;

detecting if a stored file is infected with a virus; and

saving a detected virus-infected file into a specific area designated for virus-infected files.

58. (withdrawn) A method according to claim 57, further comprising managing the detected virus infected file that is saved in the specific area.

59. (withdrawn) A method according to claim 58, further comprising deleting the detected virus-infected file.

60. (withdrawn) A method according to claim 57, further comprising encrypting the detected virus infected file that is saved in the specific area.

61. (withdrawn) A method according to claim 57, further comprising prohibiting the detected virus-infected file from executing.

62. (withdrawn) A computer readable storage medium storing a program instructing a computer to perform a method for dealing with infection of a file by a virus, the method comprising:

storing files;

detecting if a stored file is infected with a virus; and

saving a detected virus-infected file into a specific area designated for virus-infected files.

63. (withdrawn) A computer readable storage medium according to claim 62, the method further comprising managing the detected virus-infected file that is saved in the specific area.

64. (withdrawn) A computer readable storage medium according to claim 63, the method further comprising deleting the detected virus-infected file.

65. (withdrawn) A computer readable storage medium according to claim 62, the method further comprising encrypting the detected virus-infected file that is saved in the specific area.

66. (withdrawn) A computer readable storage medium according to claim 62, the method further comprising prohibiting the detected virus-infected file from executing.

67. (currently amended) An apparatus, comprising:

a virus scanner scanning a file stored in a storage device for infection with a virus; ~~and~~

a quarantining device quarantining the file from non-infected files on the storage device, when the file is infected; and

a converting device converting the quarantined file into encoded data.

68. (original) An apparatus according to claim 67, wherein the storage device comprises at least one section dedicated to storing infected files.

69. (original) An apparatus according to claim 67, wherein the quarantining device requests a user's permission before performing the quarantining.

70. (cancelled)

71. (original) An apparatus according to claim 67, wherein the file, when infected, is kept in a quarantine area on the storage device.

72. (currently amended) An apparatus, comprising:

a virus scanner scanning a file stored in a storage device for infection with a virus; and

~~an encrypting~~a converting device ~~encrypting~~ converting the file on the storage device into encoded data, if the file is infected.

73. (currently amended) An apparatus according to claim 72, wherein the file, when ~~encrypted~~converted, cannot be executed because of its ~~encrypted~~ encoded state.

74. (currently amended) An apparatus according to claim 72, wherein the ~~encrypting~~ converting device requests a user's permission before performing the ~~encrypting~~converting.

75. (currently amended) An apparatus comprising:

a storage device storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

an input device inputting a selected file with infected status; ~~and~~

a quarantining device quarantining the selected file on the storage device; and

a converting device converting the selected file into encoded data.

76. (original) An apparatus according to claim 75, wherein the selected file, when quarantined, is unable to be executed.

77. (cancelled)

78. (original) An apparatus according to claim 75, wherein the quarantining device keeps the selected file in a quarantine area on the storage device.

79. (currently amended) An apparatus, comprising:

a storage device storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

an input device inputting a selected file to be ~~encrypted~~converted; and

~~an encrypting~~a converting device ~~encrypting~~ converting the selected file into encoded data.

80. (currently amended) An apparatus according to claim 79, wherein the selected file, when ~~encrypted~~converted, is unable to be executed.

81. (currently amended) A method, comprising:
scanning a file for infection with a virus; ~~and~~
quarantining the file if infected with a virus; and
converting the quarantined file into encoded data.

82. (original) A method according to claim 81, further comprising requesting a users permission before performing the quarantining.

83. (original) A method according to claim 81, wherein the file, when infected, is kept in a quarantine area in the storage device.

84. (currently amended) A method, comprising:
scanning a file for infection with a virus;
quarantining the file from non-infected files if the file is infected with a virus; and
~~encrypting~~ converting the file into the encoded data, when infected.

85. (currently amended) A method, comprising:
scanning a file for infection with a virus; and
~~encrypting~~ converting the file into encoded data when infected with a virus.

86. (currently amended) A method according to claim 85, wherein the file, when ~~encrypted~~converted, cannot be executed because of its ~~encrypted~~ encoded state.

87. (original) A method according to claim 85, further comprising requesting a users permission before performing the encrypting.

88. (currently amended) A method, comprising:

storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

inputting a selected file with infected status to be quarantined; ~~and~~

quarantining the selected file; and

converting the quarantined file into encoded data.

89. (original) A method according to claim 88, wherein the file, when quarantined, is unable to be executed.

90. (cancelled)

91. (original) A method according to claim 88, wherein the file, when quarantined, is kept in a quarantine area in a storage device.

92. (currently amended) A method, comprising:

storing a plurality of files and a status for each file indicating whether the file is infected with a virus;

inputting a selected file to be ~~encrypted~~encoded; and

~~encrypting~~ converting the selected file into encoded data.

93. (currently amended) A method according to claim 92, wherein the ~~encrypted file~~encoded data is unable to be executed.

94. (currently amended) A computer readable storage medium controlling a computer by:

scanning a file for infection with a virus; ~~and~~

quarantining the file if infected with a virus; and

converting the quarantined file into encoded data.

95. (original) A computer readable storage medium according to claim 94, further comprising requesting a users permission before performing the quarantining.

96. (original) A computer readable storage medium according to claim 94, wherein the file, when quarantined, is kept in a quarantine area in the storage device.

97. (currently amended) A computer readable storage medium controlling a computer by:

scanning a file for infection with a virus;

quarantining the file from non-infected files, when infected; and

~~encrypting~~ converting the file into encoded data.

98. (currently amended) A computer readable storage controlling a computer by:

scanning a file for infection with a virus; and

~~encrypting~~ converting the file into encoded data when infected with a virus.

99. (currently amended) A computer readable storage medium according to claim 98, wherein the file, when ~~encrypted~~converted, cannot be executed because of its ~~encrypted~~ encoded state.

100. (original) A computer readable storage medium according to claim 98, further comprising requesting a users permission before performing the ~~encrypting~~conversion.

101. (currently amended) A computer readable storage medium controlling a computer by:

storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

inputting a selected file with infected status to be quarantined; ~~and~~

quarantining the selected file; and

converting the quarantined file into encoded data.

102. (original) A computer readable storage medium according to claim 101, wherein the selected file is unable to be executed.

103. (cancelled)

104. (original) A computer readable storage medium according to claim 101, wherein the selected file is kept in a quarantine area in the storage device.

105. (currently amended) A computer readable storage medium controlling a computer by:

storing a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

inputting a selected file to be ~~encrypted~~converted; and

~~encrypting~~ converting the selected file into encoded data.

106. (currently amended) A computer readable storage medium according to claim 105, wherein the selected file, after ~~encryption~~conversion, is unable to be executed.

107. (currently amended) A computer readable data structure controlling a computer, comprising:

a list of files stored on a storage device;

a virus status for each of the files indicating whether or not the file is virus infected; and

a quarantine status for each of the files indicated whether or not the file is quarantined, wherein the quarantined file is converted into encoded data.

108. (currently amended) A computer readable data structure controlling a computer, comprising:

a list of files stored on a storage device that are virus-infected; and

a quarantine status for each of the files indicating whether or not the file is quarantined, wherein the quarantined file is converted into encoded data.

109. (currently amended) A method comprising:

scanning a file for infection with a virus; ~~and~~

isolating the file from non-infected files, if the file is infected with a virus; and

converting the infected file into encoded data.

110. (currently amended) An apparatus comprising:

a virus scanner detecting if a file is infected with a virus; ~~and~~

a saving unit saving a detected virus-infected file into a separate storage area for virus infected files; and

a converting unit converting the virus-infected file into encoded data.